FACTORIZING LARGE NUMBERS. II

BY

D. H. G. BRETHOUWER Sr

(Communicated by Prof. J. TH. THIJSSE at the meeting of May 26, 1973)

7. INFORMATION ABOUT a, b AND x, y

During the calculations with Fermat's method we get (changing) values of k, say k_s. These latter are not integers. Through eq. (4.3.4) we can derive eq. of k_s/z and also of the pertaining a_s/b_s. It is possible to table these quantities. The result is useful for small numbers but not for large numbers. Another more promising way will be obtained through the use of recurring functions.

8. RECURRING FUNCTIONS

8.1 The *Mersenne* function $M_p = 2^p - 1 \equiv 0 \pmod{2pn+1} = 0 \pmod{b}$. Consider

$$2^p - 1 + 2pn + 1 = 2(2^{p-1} + pn) \equiv 0 \pmod{b}.$$

Consider

$$2^p - 1 - (2pn+1)^2 = 2^p - 4(pn)^2 - 2(2pn+1) \equiv 0 \pmod{b}$$

so

$$2^{p-2} - (pn)^2 \equiv 0 \pmod{b}.$$

The general function:

$$(M_i)_p = 2^{p-i} + (-1)^{i+1} \cdot (np)^i \equiv 0 \pmod{2pn+1}. \tag{8.1.1}$$

8.2 The *Fermat* function $F_n = 2^{2^n} + 1 \equiv 0 \pmod{2^{n+2}h+1} = 0 \pmod{b}$. Along the same lines as in 8.1 we get the general function:

$$(F_i)_n = 2^{2^n - i \cdot (n+2)} + (-1)^i \cdot h^i \equiv 0 \pmod{2^{n+2}h+1}. \tag{8.2.1}$$

We confine ourselves to these two functions but we remark that one can get in the same way recurring functions of e.g. $N_p = (p^p - 1)/(p-1)$ or of $2^{4^n}+1$.

8.3 What help can these recurring functions give to the factorizing of the primitive functions ($i=0$)? The principal point will be the limiting of the unknown in b (n of M_p and h of F_n). There are 3 ways; $b < z_i$ (provided $a_i > b$; is M_i or F_i positive or negative?; is M_i or F_i $>$ than M_{i+1} or F_{i+1}?

8.4 *Two examples with* M_p (M_{67} with all facts known; M_{101} with $b > 2^{35}$).

8.41 $M_{67} = 7618\ 3825\ 7287{\cdot}1\ 9370\ 7721$; $z = 121\ 4800\ 2000 = 2p \cdot 9065\ 6731 + 46$; $n = 144\ 5580$; $a/b = 3932.9266 -$; $B = 0.0127$; $np = \infty\ 2^{26.5}$. $M_0 = 2^{67} - 1$; $M_1 = 2^{66} + np$; $M_2 = 2^{65} - (np)^2$; $M_3 = 2^{64} + (np)^3$; $M_4 = 2^{63} - -(np)^4$. $b < z_0 = z$; this means $n < 9065\ 6731$; supposing $b < a_2$, $b < z_2$ or at least $n < 2^{32.5}/2p = 4532\ 8365$. Suppose $M_2 < M_3$ with the result $n > 3\ 9437$. This means $b > 2^{22.3}$ and $a/b < 2^{22.4}$. Suppose $M_4 < 0$ what means $n > 822$. The results with this recurring function: $3\ 9437 < n < < 4532\ 8365$.

8.42 Suppose, with M_{101}, $M_2 < M_3$ or $2^{99} - (np)^2 < 2^{98} + (np)^3$ with the result $np > 2^{32.67}$ and $b > 2^{33.67}$ which approximates the result mentioned by Riesel by computer-tests $b > 2^{35}$.

8.5 *Four examples with* F_n *through* $n = 5$; 6; 7 *and* 8

8.51 $(F_0)_5 = 2^{32} + 1$; $a_0 = 670\ 0417$; $h = 5$; $b = 641$

$F_1 = 2^{25} - 5$; $a_1 = 5\ 2347$;

$F_2 = 2^{18} + 5^2$; $a_2 = 409$;

$F_3 = 2^{11} - 5^3$; $a_3 = 3$;

$F_4 = 2^4 + 5^4$; $a_4 = 1$.

8.52 $(F_0)_6 = 2^{64} + 1$; $a_0 = 67\ 2804\ 2131\ 0721$; $b = 27\ 4177$; $h = 1071$.

$F_1 = 2^{56} - 1071$; $a_1 = 2628\ 1414\ 5745$;

$F_2 = 2^{48} + 1071^2$; $a_2 = 10\ 2661\ 7761$;

$F_3 = 2^{40} - 1071^3$; $a_3 = 400\ 5745$;

$F_4 = 2^{32} + 1071^4$; $a_4 = 481\ 4401$;

$F_5 = 2^{24} - 1071^5$; $a_5 = -\ 51\ 3944\ 6255$;

8.53 $(F_0)_7 = 2^{128} + 1$

$F_1 = 2^{119} - h_7$

$F_2 = 2^{110} + h^2$

$F_3 = 2^{101} - h^3$

$F_4 = 2^{92} + h^4$

$F_5 = 2^{83} - h^5$

$F_6 = 2^{74} + h^6$

8.54 $(F_0)_8 = 2^{256} + 1$

$F_1 = 2^{246} - h_8$

$F_2 = 2^{236} + h^2$

$F_3 = 2^{226} - h^3$

$F_4 = 2^{216} + h^4$

$F_5 = 2^{206} - h^5$

$F_6 = 2^{196} + h^6$

$F_8 = 2^{186} - h^7$

Through $n = 7$ and 8 the solutions are not known.

Robinson gave $b > 2^{35}$ so $h_7 > 2^{26}$ and $h_8 > 2^{25}$.

What can we tell about the limitation of h through the r functions?

8.51.1 $n = 5$; $b < z_0$ so $2^7 h + 1 < 2^{16} + 1$ and $h < 2^9$. $z_1 = 2^{12.5}$ and $h < 2^{5.5}$; $z_2 = 2^9 + f$; we have to investigate the value of f: $z_2^2 = 2^{18} + f \cdot 2^{10} + f^2$ and $z_2^2 = F_2 + r_2$; r_2 has to be positive meaning $f^2 + f \cdot 2^{10} > h^2$; if $f = h$ the condition is certainly realised but through $f = 1$ it just may be so (in this case it is) and then $h < 2^5$. Because $a_2 < b$ the condition may not be used. If $b > z_2$ it means $h > 4$. Supposing $F_3 > 0$ $h < 2^{11/3} = 12.7$; Supposing $F_3 > F_4$ leads to $h < 6.5$.

8.52.1 $n=6$; $b<z_0$ so $h<2^{24}$; $z_1=2^{28}$ and $h<2^{20}$; $z_2=2^{24}+f$ and supposing $f=1$ is sufficient (it is) through $b<z_2$ we get $h<2^{18}$. There is a stronger condition through $r_2>0$ viz. $h^2<f\cdot 2^{25}+f^2$ which means $h<2^{12.5}$ if $f=1$. Through $b<z_3$ $h<2^{12}$. Supposing $F_3<F_4$ leads to the important condition $h>2^{10}$. It is worthwhile to use this supposition: we have to test the h's from 1024 to 1071 in total 20 numbers (as we shall see through the use of various moduli many h's are excluded). The result of using these recurring functions may be illustrated by quoting "History" Vol. I, p. 377: "F. Landry, when of age 82 and after several months' labor, found that $F_6=-$".

8.53.1 $n=7$; we derive: from z_0 $h<2^{55}$; from z_1 $h<2^{50.5}$; from z_2 $h<2^{46}$. Through $r_2>0$ viz. $h^2<f\cdot 2^{56}+f^2$ and through the (speculative) value $f=1$ $h<2^{28}$, (for known higher values of n it appears that $f=1$; it is not proof but it seems very likely that in the case $n=7$ also $f=1$). The supposition $F_3<F_4$ leads to $h>2^{25}$ in accordance with the result of Robinson $h>2^{26}$. Supposing $F_3>0$ leads to $h<2^{101/3}=2^{33.66\ldots}$, but we are not sure about it (it is less strong than $h<2^{28}$). F_5 is certainly negative.

8.54.1 $n=8$; we derive: from z_0 $h<2^{118}$; from z_1 $h<2^{113}$; from z_2 $h<2^{108}$. Through $r_2>0$ and $f=1$ $h<2^{59.5}$. Robinson gave $h>2^{25}$ so $F_9=2^{166}-h^9<0$; it is possible that $F_7>0$ and in that case $h<2^{26.57}$. Certainly $F_7<F_8$ and $h>2^{23.25}$. Putting $z_4=2^{108}+f$ then $f=1$ leads to $h<2^{27.25}$ (speculative).

8.55 *The use of moduli to limit the possible values of h.*

$(F_0)_n\equiv 2 \pmod 3$ always; $b\equiv 1;\ 2 \pmod 3$. In the case $n=2w$ $h\not\equiv 2 \pmod 3$ and if $n=2w+1$ $h\not\equiv 1 \pmod 3$. Therefore one third of the numbers h can be dropped. The application of more moduli can be important. Let us consider $(F_0)=2^{64}+1$. We get

$$h\not\equiv 2 \pmod 3;\not\equiv 4 \pmod 5;\not\equiv 5 \pmod 7;\not\equiv 7 \pmod{11}.$$

If we have to test h from 1024 to 1071 only 20 values have to be considered. If a computer is used the "sieving" can possibly be programmed.

8.6 *Approximation of a/b*

Each function M_p or F_n has an a/b which can be the condition underlying the application of multiplication to get the utmost from contracting. Now a/b is equal to the function divided by b^2. If there are bounds of b we can get also bounds of a/b. In principle $b=U+1=U(1+U^{-1})$. Since U^{-1} will be very small, instead of dividing by $1+U^{-1}$ we may multiply by $1-U^{-1}$. The same is true for squares.

8.61 Two *examples* with F_n. If $n=6$ $(F_0)_6=2^{64}+1$;

$$b=h\cdot 2^8+1=h\cdot 2^8(1+h^{-1}\cdot 2^{-8});$$

$$a/b=(2^{48}\cdot h^{-2}+h^{-2}\cdot 2^{-16})\cdot(1-2^{-7}h^{-1}-2^{-16}\cdot h^{-2})=2^{48}\cdot h^{-2}-2^{41}\cdot h^{-3}-\text{negligible}.$$

Using the results of 8.52.1: $2^{10}<h<2^{12}$ we put $h=2^{10+v}$ (with the strong surmise $v<2$ and $a/b=2^{28-2v}-2^{11-3v}$.

$$B=(a/b)^{\frac{1}{2}}/(z/8)^{\frac{1}{2}}=2^{\frac{1}{2}(28-2v)}(1-2^{-17-v})^{\frac{1}{2}}/2^{14.5}(1+2^{-32})^{\frac{1}{2}}=2^{6.5-1.5v}$$

(main part). Taking $x_0=2$ we get through eq. (6.21.2):

$$2^{29-2v}-2^{12-3v}-2^{7-1.5v}<y_0<2^{29-2v}-2^{12-3v}+2^{7-1.5v}$$

(in reality $h=1071=2^{10.065}$ so $v=0.065$). We use these results in 9. If $n=7$ we get along the same lines: $a/b=2^{110}\cdot h^{-2}-2^{102}\cdot h^{-3}$. Using the results of 8.53.1: $2^{26}<h<2^{28}$ we put $h=2^{26+w}$ (with the strong surmise $w<2$ and $a/b=2^{58-2w}-2^{24-3w}$; $B=2^{13.5-1.5w}$. Taking $x_0=2$ we get through eq. (6.21.2):

$$2^{59-2w}-2^{25-3w}-2^{13.5-1.5w}<y_0<2^{59-2w}-2^{25-3w}+2^{13.5-1.5w}.$$

9. Method of getting "adapted" multipliers (*unknown* a/b)

9.1 In 6.21 it was shown with M_{67}: $x_0'=1$ and $y_0'=3933$. Using successively the multipliers 3, 5, 7 – 3933 the number of experiments to get the solution is 1966. This method seems attractive but if a/b is not small and the bounds are wide the procedure fails.

If we like to use the method of successive multipliers it will be wise simultaneously to use the procedure of divisions by successive primes of the wanted form.

9.2 We will now show the method of getting "adapted" multipliers. If and only if $k_{xy}=(K_{xy})_G$ $x=x_0$ or x_0' and $y=y_0$ or y_0'. Mathematically written:

$$(K_{xy})_G=K_{xy}-G\cdot[K_{xy/G}]. \tag{9.2.1}$$

9.21 *Numbers of Mersenne*

Since the value of $y-x$ is unknown we take $G=2p$ (see 5.6). Per definition $K_{xy}=(xM_p+y)/2-z_{xy}$ and through $M_p=2pQ+1$ $K_{xy}=pQx+$ $+(x+y)/2-z_{xy}$. Always $Q\equiv 1(\text{mod } 2)$.

$$(K_{xy})_{2p}=(px)_{2p}+((x+y)/2)_{2p}-(z_{xy})_{2p}. \tag{9.21.1}$$

Due to eq. (9.2.1) we write:

$$(K_{xy})_{2p}=px+(x+y)/2-z_{xy}-2p\cdot[px/2p+(x+y)/4p-(z_{xy})/2p].$$

Through $k_{xy}=(K_{xy})_{2p}$ we get $2(z_{xy}+k_{xy})=2px+x+y-4p$. $[-]$.

Calling

$$z_{xy}+k_{xy}\equiv c(\text{mod } 2p) \tag{9.21.2}$$

$$y\equiv 2c+x(2p-1)(\text{mod } 4p). \tag{9.21.3}$$

In this eq. $y=y_0$ or y_0' and $x=x_0$ or x_0'; c can have the values from 0 to $2p-1$; with a chosen value of x, a series of y dependent on the added number of $4p$ belongs to each value of c. Through each y (and x) one can check (see 9.) whether there is a solution through x_0y_0 or $x_0'y_0'$. Getting ahead of the complete elaboration we give 2 examples to elucidate the method.

EXAMPLE 1. Through $p=11$ and $x=1$ there is no solution through $c=0$ to 12; if $c=13$ $y\equiv 3 \pmod{44}$ and $c=14$ $y\equiv 5 \pmod{44}$; $y_0=3$ or 5 are solutions; if $c=15$ $y_0'=7$ etc.

EXAMPLE 2. Through $p=67$ and $x=1$ with $c=24$ we get $y\equiv 181 \pmod{4p}$; the 15th $y=3933=y_0'$ is a solution.

9.21.1 We have to consider which value of y we use as a maximum through each c. Calling $y_1=2c+x(2p-1)$ then $y\equiv y_1 \pmod{4p}$; $y_{\max}=$ $=y_1+4pA_1$ and $y_{\max}/x=y_1/x+4pA_1/x$; $y_{\max}/x$ has to be larger than a/b. If we take $A_1/x=A$ then it means that we suppose $y_1/x<a/b<y_1/x+4pA$.

9.22 *Numbers of Fermat*

Along the same way as in (9.21) we get $G=2^{n+2}$ and

$$y\equiv 2c-x \pmod{2^{n+3}} \tag{9.22.1}$$

c can have the values from 0 to $2^{n+2}-1$.

It is possible to consider other functions but we restrinct ourselves to these two. In the next summary we call the functions M_p and F_n: P.

9.23 *Summarizing the necessary equations*

$$z^2=P+r \tag{9.23.1}$$

$$z_{xy}^2=xyP+r_{xy} \tag{9.23.2}$$

$$R_G=R-G\cdot[R/G] \tag{9.23.3}$$

R may be K_{xy}; px; $(x+y)/2$; z_{xy}.

$$z_{xy}+k_{xy}\equiv c \pmod{G} \tag{9.23.4}$$

$$y\equiv 2c+x(2p-1) \pmod{4p} \text{ or } y\equiv 2c-x \pmod{2^{n+3}} \tag{9.23.5}$$

$$y_1=2c+x(2p-1) \text{ or } y_1=2c-x \tag{9.23.6}$$

$$y_{\max}=y_1+xA\cdot 2G \text{ (Choosing } A) \tag{9.23.7}$$

$$z_{xy}+(K_{xy})_G=C \tag{9.23.8}$$

$$z_{xy}+C=C_1 \tag{9.23.9}$$

$$V=C^2-xyP=r_{xy}+(K_{xy})_G\cdot C_1 \tag{9.23.10}$$

$$B=(a/b^{\frac{1}{2}})/(z/8)^{\frac{1}{2}} \tag{9.23.11}$$

$$s_q>(y_q-x_q\cdot a/b)^2/x_q\cdot G\cdot B^2-(1+(K_q)_G)/G \tag{9.23.12}$$

1st qualification: $s_{xy}=0$; x, $y=x_0$, y_0 or x_0', y_0' and $k_{xy}=(K_{xy})_G$
2nd qualification: $s_{xy}=s_q>0$; x, $y=x_q$, y_q and $k_q=(K_{xy})_G+s_q\cdot G$.

9.24 *Method of testing*

9.24.1 *Testing whether an x, y from eq. (9.23.5) is x_0, y_0 or x_0', y_0'*
9.24.11 Determine z_{xy} and r_{xy}. If the latter is a square $x, y=x_0, y_0$.
9.24.12 If r_{xy} is not a square determine $(z_{xy})_G$ through eq. (9.23.3).
9.24.13 Determine $(K_{xy})_G$ through eq. (9.23.3).
9.24.14 Is V (eq. (9.23.10) a square? If affirmative $x, y=x_0, y_0$ if $(K_{xy})_G=0$; $x, y=x_0', y_0'$ if $(K_{xy})_G \not\equiv 0$. If negative test another couple of x, y or test x_q, y_q.

9.24.2 *Testing whether an x, y is x_q, y_q*
9.24.21 After the procedure of .11 to .14: is $V+2G\cdot s_q\cdot(C+s_q\cdot G/2)$ a square? (later on we shall examine how many values of s_q we want to use). If affirmative the problem is solved. If negative test other values of s_q.

9.25 *Elaboration of the method*

There are two ways of solving the problem. We can take a value of x and through this value we have the values of y_1 which result from $c=0, 1-(G-1)$. The next value of $y=y_1+4p$ and so on. In this way a "card" of a chosen x is produced. It is also possible to start with a value of c and give x the values 1, 2 etc. In this way a "c-card" is produced. Hereunder we give some examples of this procedure which is called the "cards-method". We take some numbers of Mersenne; $A=20$.

Method 1 *by "x-cards"* with $M_{67}=2^{67}-1$ $(p=67)$

$p=67$	$x=1$			
c	y_1	$y\equiv y_1 \pmod{4p}$		y_{max}
0	133	401	.....3885.....	5493
1	135	403	3887	5495
'	'	'	'	'
24	181	449	*3933*	
'	'	'		
133				

$x_0'=1$ and $y_0'=3933$

Number of tests: by each c-value $1+20x=21$
by c from 0 up to 23: $24\cdot 21=504$
by $c=24$ 15
Total *519*

Method 2 by "c-cards" ($p=67$)

By $c=0$ we need only $x=1$ as a sufficient and necessary condition. The number of tests is 21.

$p=67$	$c=1$			
x	y_1	$y \equiv y_1 \pmod{4p}$		y_{max}
1	135	403	.....	5495
2	268	536		10988
'	'	'		
28	3726		..... *11 0122*	

$x_0 = 28$ and $y_0 = 11\ 0122$

Number of tests: by $c=0$ 21

by x from 1 up to 27 $x_{max}+20\sum_{1}^{27} x = 7587$

by $x=28$ 398

Total = 8006

REMARK: Through $c=111$ $x_0=27$ and $y_0=10\ 6189$.

If we consider M_{79} the third prime of the form $2pn+1=2687$ which is a divisor; therefore we consider $M'_{79}=M_{79}/2687$.

Method 1 by "x-cards" we learn that through $x=1$ up to 6 inclusive ($A=20$) there is no solution; $x_0'=7$ and $y_0'=38581$. It requires 8 1104 tests.

Method 2 by "c-cards": through $c=1$ we get $x_0'=18$ and $y_0'=9\ 9208$. It requires 3404 tests. Remark: through $c=115$ $x_0=23$ and $y_0=12\ 6765$.

9.26 *Discussion of the number of tests in comparison with other methods*

9.26.1 $p=67$ If we test classically by division of $2pn+1$ i.e. $2p+1$, $6p+1$, $8p+1$ etc. the divisors have to be prime; if they are larger than 10^7 we are in the dark. Although it is recommendable also to divide by the nearest divisor smaller than z and then go on downwards the trouble is that there is no certainty whether the numbers are prime or not. If one uses a computer this trouble hardly seems to play a role.

Through M_{67} $b=1\ 9370\ 7721=2p\cdot 144\ 5580+1$. In this case $n \not\equiv 1 \pmod 3$ so we may consider $2/3\cdot 144\ 5580=96\ 3720$ as the number of tests using the "division-method". The test itself is simple and short.

If we factorize M_{67} by the – contracted – method of Fermat there is $k \equiv K_{8p^2} \pmod{8p^2}$ which means $k=2\ 7224+s\cdot 8p^2$ and $s=1027\ 1440$, the number of tests (steps). The test itself takes more time because we have to answer the question whether $(z+k)^2-M_p$ is a square.

In the third place we found that by multiplying by 3, 5 – 3933 we needed 1966 tests. Further on we dealt with the question of larger moduli in 4.4. So we make the following comparison:

Number of tests:	k-method	1027 1440
	division method	96 3720
	method with larger moduli	4 0320
	c-card method ($c=0$; 1)	8006
	multiplying in succession	1966
	x-card method ($x=1$)	519

9.26.2 $p=79$ $b'=2$ 0202 9703 $=2p\cdot 127$ 8669 $+1$; number of tests $2/3\cdot 127$ 8669 $=85$ 2446. Through the k-method $s=1085$ 2587; $x_0'=7$ and $y_0'=3$ 8581; $x_0'y_0'=27$ 0067; the method by multiplying in succession would ask 13 5033 tests. Comparison:

Number of tests:	k-method	1085 2587
	method with larger moduli	576 5760
	division method – about	85 2446
	multiplying in succession	13 5033
	x-card method ($x=1$, 2, 3, 4, 5, 6, 7)	8 1104
	c-card method ($c=0$; 1)	3404

CONCLUSIONS: See 10.

9.27 *The possibilities of reducing the number of tests with the card-method*

9.27.1 In 9.21.1 we supposed $a/b>y_1/x$. A good estimation of a/b can reduce the number of tests. From eq. (6.2.2) follows:

$$((y-x\cdot a/b)/x^{\frac{1}{2}})^2<(k_{xy}+1)\cdot(a/b)^{3/2}/(z/8).$$

Calling $(y-x\cdot a/b)/x^{\frac{1}{2}}=T$ we get

$$a/b>(z/8)^{2/3}\cdot T^{4/3}/(k_{xy}+1)^{2/3}. \tag{9.27.1}$$

We remark about the value of $y-x\cdot a/b$ that $[a/b]$ can be odd or even. Suppose (from M'_{79}) $a/b=5511.5219$ then $[a/b]=5511$. If $x=2$ $xa/b=$ $=11023.0438$ and $[xa/b]=11023$; if $x=4$ $xa/b=22046.0876$ and $[xa/b]=$ $=22046$. It is essential that x and y are both odd or both even; further y has to be as near as is possible to $[xa/b]$. So in the case $x=2$ $y=11024$ and $y-xa/b=0.9562$; if $x=4$ $y-xa/b=0.0876$. There can be the same situation with x odd.

CONCLUSION: If y is as near to $[xa/b]$ as possible, then due to the fact that x and y both have to be odd or both even, the maximum of $y-xa/b=1$; the minimum can be in the neighbourhood of 0. Some calculations in different cases showed that a/b is much too large taking $y-xa/b=1$.

9.27.2 Looking after $B=(a/b)^{\frac{3}{2}}/(z/8)^{\frac{1}{2}}$ we solve a/b:

$$a/b=(z/8)^{2/3}\cdot B^{4/3}. \tag{9.27.2.1}$$

Through $b = \sim z \cdot (a/b)^{-\frac{1}{2}}$ we get $b = \sim 2z^{2/3}/B^{2/3}$ and the conclusion is the larger B the smaller b. Some values of B: through M_{11} 1.15; M_{23} 25.4; M_{37} 315; M_{59} 28; M_{67} 0.0127; M'_{79} 0.01474. In principle we may say that with large B the method of dividing by successive primes of the right form will be the best. But when call we B large?

Suppose $x_0 = 1$ and $y = y_0$; $k_{x_0 y_0} = 0$ and $a/b - B < y_0 < a/b + B$ so if $B = 1$ at least there will always be $x_0 = 1$ and an y_0. It is known through M_{101}: $b > 2^{35}$ and $a/b < 2^{31}$ so $B < 0.7$.

If we choose for B a certain value there is the risk of choosing too large a value and there can be no success when using the card method. The same is true when $y_{\max}$ is chosen too small.

9.27.3 By using x_0', y_0' B can be smaller to get a sure result. In that case taking $x_0' = 1$ there is:

$$a/b - B(k_{x_0' y_0'} + 1)^{\frac{1}{2}} < y_0' < a/b + B(k_{x_0' y_0'} + 1)^{\frac{1}{2}}$$

and there is always a solution if $B(k_{x_0' y_0'} + 1)^{\frac{1}{2}} = 1$. Since the minimum of $k_{x_0' y_0'} = 1$ and the maximum $G - 1$ (in the case of M $2p - 1$) we get a good result if $B > 0.707$.

9.27.4 There is one striking point in the cards-method. Sometimes the use of x-cards is far more advantageous than the use of c-cards but it may also be otherwise. One can see that by viewing the examples.

$p = 67$; x-card number of tests 519; c-card 8006.
$p = 79$; x-card 8 1104; c-card 3404.

As far as I know it seems impossible to see beforehand which method in a certain case will be the most favourable. Using the c-method it can be necessary to produce $2p$ c-cards; and with every card there is the problem which value of $x_{\max}$ one has to take. Using the x-card it may be necessary to use all the values of c from 0 to $G - 1$.

9.27.5 Anyhow it seems advisable to use $x = 1$. The use of the larger x has the advantage that the value of $T_{\max}$ will be smaller. If one compares the values of T through $x = 1$ and through an even value of x say $x = 4$ it may happen that one of them gives no solution and the otherone leads to a solution. I am inclined to propose *not to use the c-cards* and to use $x = 1$ and $x = 4$ in every case; if there is no result then a higher value of x e.g. $x = 7$; 10.

9.27.6 We have to pay attention to the use of x_q and y_q. In the case M'_{79} we calculated ($[a/b] = 5511$): $x_q = 1$; $y_q = 5511$; $s_q = 7$. $x_q = 1$; $y_q = 5513$; $s_q = 63$. $x_q = 1$; $y_q = 5509$; $s_q = 184$. If we take $x_q = 4$ and through $c = 123$ $y_q = 22046$ with $s_q = 1$. So extending the method of testing by $s_q = 1$ will be well paid. The number of tests through $x = 1$ will be $158 \cdot 21 = 3318$; through $x = 4$ by each c-value $1 + 4 \cdot 20 = 81$; by c from 0 to 122 inclusive $123 \cdot 81 = 9963$; by $c = 123$ the number of tests is 68. So in total 13349 extended tests. This number can be compared with 81104 ($x = 1$ to 7).

9.27.7 Through the x-card method we may take c alternately: beginning with $c=0$ and $c=2p-1$; $c=2$ and $c=2p-1$ and so on. In the example of the previous point we get to $c=123$ after having used 69 values of c the number of tests is $69 \cdot 81 = 5589$ and 68 for $c=123$ the total is 5657 against 10031 in the normal way of c successively. The alternative method asks for the same amount of tests when there is no solution; if a certain x leads to a solution through $c<p$ then we have done superfluous work.

9.27.8 If we would use many values of $s_q=1$; 2; 3 etc. the tests itself would take more and more time. If one has a good calculating-machine the tests are done in a relatively short time; it seems to me that the programming for a computer to work through the x-card method, included the tests, will be no obstacle.

10. Conclusions

10.1 After the (only) two examples of 9.26 it seems that the cards-method is attractive.

10.2 It will be advisable to study this method, especially the reducing of tests, on a larger scale.

10.3 The application to other functions e.g. the numbers of Fermat will also require research (see 9.22).

10.4 The use of the recurring functions seems advantageous. The different i-functions have the same divisor b; in this respect a research will be advisable.

10.5 The "tentative method" needs more investigation.

LITERATURE

I 1 I Trost, Ernst, "Primzahlen", 1953.

I 2 I Dickson, L. E., History of the Theory of Numbers, volume I, II and III.

I 3 I Riesel, H., "Mathematics of Computation", Vol. 16, No. 80, p. 478–482, October 1962.

I 4 I Lehmer, D. H., Guide to Tables in the Theory of Numbers, reprinted 1961.

I 5 I Maennchen, P., "Zerlegung grosser Zahlen", Unterrichtsbl. Math. Naturwissenschaft 44, 84–92, 112–122 (1938).

I 6 I Hütte, Hilfstafeln zur Ermittlung von Räderübersetzungen; 8 Auflage, Berlin, Verlag von Wilhelm Ernst & Sohn. 1965.

I 7 I Ore, Oystein, Number Theory and its History. 1948.

I 8 I Hardy, G. H. and E. M. Wright, An Introduction to the theory of numbers (fourth edition 1959).

I 9 I Schuh, F., Leerboek der elementaire Rekenkunde, Deel I; P. Noordhoff – 1919 – Groningen.

I 10 I Hildebrand, F. B., Introduction to numerical Analysis; Mc fraw Hill book Company Inc. 1956.